Adrian Valencia

CYSE 200T

Professor Kirkpatrick

7 November, 2025

SCADA Systems Write-up

BLUF

Within critical infrastructure systems, many vulnerabilities and risks are overlooked through Supervisory Control and Data Acquisition (SCADA). They overlook infrastructure systems and facilities, such as water treatment plants, airports, and other operations that generate large amounts of data. As a result of the mass of information held, many vulnerabilities and risks persist within the networks. In essence, SCADA security is a vulnerability that needs constant attention to strengthen its infrastructure.

Vulnerabilities of SCADA Systems

The objective of SCADA networks is to coordinate and automate, which leads to vulnerabilities in both a cyber and physical security perspective. For example, in the SCADA Systems article, it goes over the generations of SCADA and the methods used, like proprietary protocols and isolated systems. In the present SCADA, the new vulnerabilities and risks that arise are through the new methods of the Internet and Ethernet methods used. The two bring along problems such as malware, authorization issues, and other general issues that come along with them.

Solutions to Vulnerabilities

Two major problems that are discussed within the article are the attacks of unauthorized users on the control software and the networking communication instability. Unauthorized access to systems like healthcare could be the reason why records can become unavailable in an instant (SentinelOne, 2025). However, through response and multi-factor authentication, the access can be fixed and controlled within the department. Furthermore, firewalls and VPNS are common implementations that are in the SCADA protocols that keep systems maintained at a level.

Additionally, having updates with constant patches allows for networks and other troubleshooting issues to be more stable and consistent. Through network isolating, the surface area of attack needs to be more widespread, adding a layer of security. Adding to it, the access controls and physical security are things to be constantly monitored that will secure the systems to a further level.

Conclusion

In conclusion, SCADA systems are a pillar of security within infrastructure that are monitored in many ways. Cybersecurity protocols and measures help support the ideals with control over the systems that lead to the safety of organizations and companies. Through SCADA, many roles in cybersecurity are addressed that require constant adaptation to risks and threats that are imperative to look out for.

References

SentinelOne 2025 -

https://www.sentinelone.com/cybersecurity-101/cybersecurity/what-is-cyber-infrastructure/

SCADA Article -

https://docs.google.com/document/d/1VnMlL2YmcW5Jg4MdDa1dt5fJpmQM0KVH/edit